

Appendix 2

自動車分野の機能安全規格に対処する実務ガイドライン「MISRA-SA」を知る

自動車業界の要請はCコーディング・ガイドラインから安全性解析へ

二上貴夫

ここでは，自動車の業界団体であるMISRA（The Motor Industry Software Reliability Association）が策定しているガイドライン「MISRA安全性解析（MISRA-SA）」について解説する．MISRA-SAは，2008年に策定される予定の機能安全規格「ISO 26262」に適合した開発実務を実現するためのガイドライン（指南書）という位置付けにある．（編集部）

MISRA（The Motor Industry Software Reliability Association；ミスラまたはミズラと発音）と聞くと，皆さんは，自動車業界で用いられるCプログラミング・ガイドライン「MISRA-C」を思い浮かべるかもしれません．実は，MISRAとは，ガイドラインを作成している業界団体の名称であって，ガイドラインそのものではありません．

MISRAは，自動車関連ソフトウェアの安全性や信頼性に関わる研究と，ガイドラインの作成を行っています．

「MISRA Safety Analysis（MISRA安全性解析；以降，MISRA-SAと表記）」も，MISRAが作成しているガイドラインの一つです．

● 自動車分野における機能安全対策の実務指針

MISRA-SAは，自動車および自動車のサブシステムで安全性に関連するソフトウェアを開発する技術者のための，安全性解析に関するガイドラインです．現在は最終ドラフト版が配布され，世界各国からコメントを集めているところです(1)．これが終了すると初版が発行されます（早ければ，2006年末までに発行される予定）．

自動車業界では今世紀に入ってから，完成車であれECU（electric control unit）部品であれ，搭載する組み込み制御ソフトウェアの信頼性を明確に示すことを求める声が高くなってきました．この要請に応えるため，Cソース・コードの信頼性を検証する手段として，MISRA-Cが各国の自動車メーカで採用されたという経緯があります．日本はこの要請に的確に対応して，ソース・コード・レベルでの品質向上を果たしました．そして次の課題が，安全性解析というわけです．

安全性検証という観点では，IEC 61508とその派生規格が今後の国際標準になると言われています．自動車分野における派生規格としては「ISO 26262」が2008年に策定される予定です．MISRA-SAは，この規格を満足する開発実務を実現するための指南書という位置付けになります．

規格には，どの工程でどういった文書（ドキュメント）をこうした方法論で作りなさい，という定義が並んでいます．例えば，航空宇宙産業でのキャリアのある技術者ならば，規格を読めばどうすればよいかが分かりますし，開発組織自体がその定義を満たす形になっているものです．しかし，一般の自動車産業では，航空宇宙産業などと比較して発展の仕方が異なったため，技術者がエンジニアリング・プロセスと計算根拠を学ぶ必要があります．さらに，定式化された安全性解析についても知らない技術者が多く存在します．こうした自動車産業の実情を踏まえて発行されるのが，MISRA-SAです．いわば，これから生まれるISO 26262に対処するための，実務上のガイドラインという位置付けになります（**図1**）．

筆者がMISRAの存在を知ったのは1996年でした．それ以来10年間，彼らの活動を観察する機会（一種の幸運）に恵まれました．MISRAは1900年代の初頭から，産学連携で来るべき自動車産業の在り方を研究し，時代の要請に合わせてガイドラインを発行してきています．これは一朝一夕ではまねできないものです．幸い，日本はMISRA-Cの策定にいろいろ貢献しているので[注1]，MISRA-SAに関しても優先的に情報を提供してもらえる立場にあります．本稿もMISRAの了承の下に，ドラフト版に基づいて解説しています．

KeyWord　MISRA-SA，安全性解析，機能安全，IEC 61508，ISO 26262，許容リスク

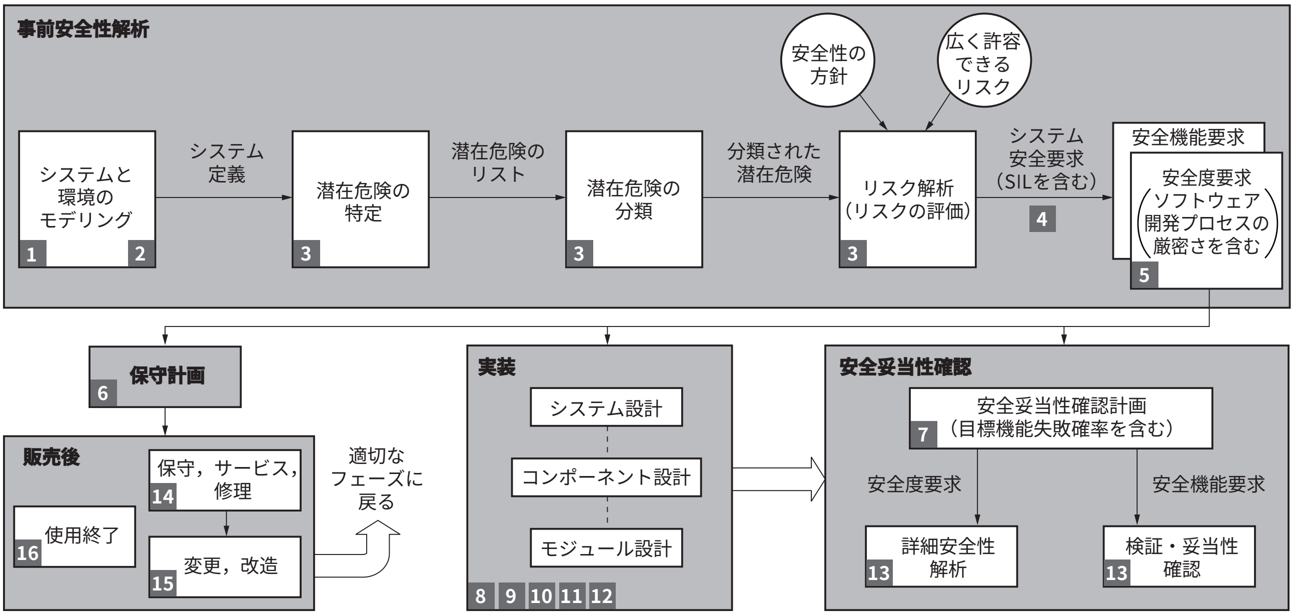


図1　MISRA-SAのライフ・サイクル（ドラフト版）
黒四角の数字は，IEC 61508のライフ・サイクルにおけるフェーズとの対応を示している．

● MISRA-SAの概略

MISRA-SAについて知りたい方は，何はさておき原文を読むのが一番です[注2]．ただし，99ページの英文を一気に通読できる気力と語学力が必要です．そこまで労力（コスト）をかけることにためらいがある方には，本稿を読んで全体の骨子を理解しておき，翻訳版が出てから詳細を理解する，という方法をお勧めします．

以下に，ドラフト版の概略（要約）を示します．

● 第1章：本書の目的，IEC 61508やDEF STAN00-56との関係

MISRA-SAを策定したメンバはIEC 61508の策定にもかかわった人たちであり，ISO 26262の委員でもあります．また，MISRA-Cによるコード品質改善も推進してきたわけですから，標準ルールを作るだけでは現場に適用するのは難しいことを理解しています．このため，過去10数年の経緯を解説して，MISRA-SAの位置付けを明確にしています．

● 第2章：安全性保障の開発文化，安全性を扱うための概念

安全性マネージメントという言葉を用いて，製品開発の中で安全性を明示的に設計に取り込むための仕組みや考え方を解説しています．この仕組みがあれば，開発組織において国際標準が要請するさまざまなドキュメントを合理的に作成できるはずです．

● 第3章：従来のV字開発プロセスに安全性保障を加味する

V字開発プロセスは，よく知られているところです．このプロセスに対して，安全性を保障するための工程をどのように加えるべきかが解説されています．

● 第4章：事前安全性解析

事前安全性解析とは，システム開発の事前（もしくは初期）に行うべき製品の安全面の解析作業です．特にプログラミング可能な電子デバイス（いわゆるマイコンなどのこと．IEC 61508で“programmable electronic”と表現されている．PEと略す）を新規に用いて製品を開発する場合に，そのリスク評価を含めて解析を実施する方法が記述されています（具体的な項目については，**図1**に示す「事前安全性解析」ブロックの中の記述を参照のこと）．

● 第5章：詳細安全性解析

詳細安全性解析とは，安全性解析をより具体的に記述したものです．「システム設計」，「類推的解析と演繹的解析」，「結果解析」などの項目が含まれます．

● 第6章：参考文献

● 付録 A. システムと潜在危険（hazard）特定モデル
B. What If解析

注1：ここでは主に，自動車技術会のテクニカル・ペーパ，自動車工業会のサブセット・ガイドライン，2002年4月に発足したMISRA-C研究会のMISRA-C解説書などを指している．MISRA-C研究会は現在，NPO法人であるSESSAME（組込みソフトウェア管理者・技術者育成研究会）のワーキング・グループとして活動している．
注2：ドラフト版は一般には公開されていない．興味のある方は直接MISRAに掛け合うか，SESSAME事務局に連絡してみることをお勧めする．

C. HAZOP実施への助言

D. リスク・モデルとリスク評価

E. 制御性パラメータと分類

F. FMEA実施への助言

G. FTA実施への助言

付録として30ページを費やして，安全性設計の分野で使われている技法を自動車に適用するための示唆が書かれています．

● 安全性計算の根拠と背景

機能安全の基本的な前提は，起きていない事象を予防することです．この意味で，プログラマの日常的なデバッグ作業とは本質的に異なる計算の上に成り立っているのが機能安全です．MISRA-SAは，そうした安全性計算の根拠についても述べています．

1）1台の自動車をシステムとみなして安全性を計算

MISRA-SAは，1台の自動車をシステムとみなした安全性計算と開発を狙いにしています．つまり，自動車を群ととらえた，ITS（intelligent transport systems；高度道路交通システム）的な全体の安全保障という概念は扱っていません．MISRA-SAを策定した中心メンバは，欧州交通システムの基本アーキテクチャを策定した人たちですが，この領域は需要や実験データの量などの理由から，扱える範囲に入れていないと思われます．

2）欧州の社会常識・見解を定量化

MISRA-SAは安全性議論の根拠として，英国における交通事故死者や各種の社会的安全性研究の結果を引用しています．基本は，以下に示すいくつかの公共許容リスクの基準（これだけの危害が出てもやむを得ないと割り切れる上限の基準）から推定しています．

- 英国の年間交通事故死確率は10^{-4}オーダである（日本も同じ）．また，そのほとんどが，人間の不注意や操作ミスなどに起因している
- ドイツにおける許容リスクの判断基準「MEM（Minimum Endogeneos Mortality）」において，ほかの産業における最小自然致死基準（例えば，原子炉周辺で生活した場合に被爆によって死亡する確率の上限）のうち技術的な原因（例えば，原子炉配管の疲労による破断予測の不一致など）による確率は10^{-5}と上限を定めている
- 英国の健康安全局（HSE：Health and Safety Executive）は（個人への受益性を加味して）10^{-6}と設定している

これらの基準から，潜在危険が事故につながる危険性を加味して，リスク・レベルと時間当たりの障害（危険側故障）発生の許容確率を示しています．

その結果，MISRA-SAではプログラミング可能な電子デバイス（PE）システムにおいて許容できるリスクを10^{-4}と定義しています．しかし，これでは許容リスクぎりぎりで安全性計算をしてしまう可能性が高く，計算ミスなどにより社会的に許容できない自動車がちまたを走り回ることも考えられます．また，日本の品質管理は，欠陥ゼロ（zero defect）を目標に改善を行ってきたので，最初から高めの目標を持つべきであるという声もあります．

参考・引用*文献

(1) Guidelines for the Safety Analysis of Vehicle Based Programmable Systems（Draft Post Public review Rev. 13），July 2006.

ふたがみ・たかお
（株）東陽テクニカ

<筆者プロフィール>
組み込みシステムやソフトウェアの開発関連のコンサルティング，開発ツールの応用をしごととしている．特に，自動車の組み込みソフトウェアの信頼性向上と標準化，SESSAMEやTOPPERSプロジェクトなどの技術者教育用の実験・カリキュラム開発などに力を入れている．